UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/944,739	08/31/2001	Poorvi L. Vora	10004408 -1	2015

7590 02/23/2006

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
OYEBISI, OJO O	
ART UNIT	PAPER NUMBER
3628	

DATE MAILED: 02/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/944,739	**Applicant(s)** VORA ET AL.	
	Examiner OJO O. OYEBISI	**Art Unit** 3628	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 May 2004*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 August 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *08/31/01*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-25 are rejected under 35 U.S.C. 102(b) as being anticipated by Krsul et al (Krsul hereinafter, US PAT: 5,839,119).

Re claim 1. Krsul discloses a method by an anonymity service provider (i.e., seller/merchant) for anonymous acquisition of a digital product by an entity, the method comprising: receiving, from the entity, a plurality of acquisition-related variables necessary for the entity to acquire the digital product (i.e., determining the amount of money adequate for the transaction, and the seller with whom the buyer wants to do business, see col.5 lines 60-67); splitting at least some of the plurality of acquisition-related variables into a corresponding at least one set of variable secret shares (i.e., splitting the electronic tokens into half, see col.7 lines 45-55, also see abstract); for each of the at least one set of variable secret shares (i.e., electronic tokens), sending the set of variable secret shares to a set of shareholders for long-term storage of the acquisition-related variables (the financial service provider assigns half of the electronic to the buyer and the other half to the seller, see col.2 lines 20-50, also see abstract); and fulfilling acquisition of the digital product by the entity based on the plurality of acquisition-related variables such that a provider of the digital product is unable to identify the entity (i.e., providing anonymity to buyer, and preventing sellers from building a dossier about the buyer, see col.6 lines 40-48) (see col.2, lines 20-50, also see abstract).

Re claim 2. Krsul further discloses the method of claim 1, further comprising: assigning a transaction identification to the plurality of acquisition-related variables (i.e., bank assigns a unique identifier, see col.8 lines 35-40); and associatively storing the transaction identification with identifications of shareholders of each set of shareholders (see col.8 lines 40-55).

Re claim 3. Krsul further discloses the method of claim 1, wherein a first set of shareholders receive a first set of variable secret shares and at least a second set of shareholders receive at least a second set of variable secret shares (i.e., the financial service provider assigns half of the electronic to the buyer and the other half to the seller, see col.2 lines 20-50, also see abstract).

Re claims 4 and 5. Krsul further discloses the method of claim 3, wherein the first set of shareholders is not identical to the at least second set of shareholders (i.e., the financial service provider assigns half of the electronic to the buyer (first set of shareholder) and the other half to the seller (the second set of shareholder), see col.2 lines 20-50, also see abstract. Note that buyers and sellers are not identical with no common members).

Re claim 6. Krsul further discloses the method of claim 3, wherein the first set of shareholders is identical to each of the at least second set of shareholders (i.e., bank may assign the seller (one set of shareholder) all of the first token halves (shares), and all of the second token halves (shares), or some combination of the first and second token halves, so long as neither the seller nor buyer receives both halves of the electronic token, see col.8, lines 46-53).

Re claim 7. Krsul further discloses the method of claim 1, wherein the plurality of acquisition-related variables comprises an entity identification corresponding to the entity and a digital product identification corresponding to the digital product (i.e., unique identifier see col.8, lines 35-45).

Re claim 8. Krsul further discloses the method of claim 7, wherein the plurality of acquisition-related variables further comprises a purchase price corresponding to the digital product (i.e., the amount of money adequate for the transaction, see col.5 lines 60-65).

Re claim 9. Krsul further discloses the method of claim 8, wherein the plurality of acquisition-related variables comprise credit information, and wherein fulfilling acquisition of the digital product further comprises: verifying credit of the entity with a credit agency based on the entity identification, purchase price and credit information such that the credit agency is unable to identify the digital product or the provider of the digital product (i.e., If bank 18 does not find a match, the seller is attempting to double spend the token, and bank 18 will not credit the seller for that electronic token. On the other hand, if the serial number of the electronic token matches a session serial number remaining in the relevant database entry, bank 18 removes the session serial number of the redeemed electronic token from the database entry and advances to step 1066. Bank 18 may also detect double spending using other approaches.

Whatever approach is taken, bank 18 needs to ensure that it only honors an electronic token once. Once bank 18 determines that an electronic token is valid, however that is done, during step 1066 bank 18 increases the sum due to seller 17 by the amount of the electronic token. That done, bank 18 continues executing steps 1063 through 1066 until all of the seller's electronic tokens have been processed. When that occurs, during step 1068 bank 18 informs seller 17 of the credit to be given him and how that credit will be given to him, see col.11 lines 20-40).

Re claim 10. Krsul further discloses the method for an anonymity service provider to support anonymous acquisition, by an entity, of a digital product, the method comprising: receiving, from the entity, an acquisition request comprising a digital product identification corresponding to the digital product and an entity identification corresponding to the entity (i.e., unique identifiers and session serial numbers, see col.8, lines 30-45, also see col.7, lines 17-45); assigning a transaction identification that uniquely identifies the acquisition request (i.e., unique identifier, see col.8 lines 30-45); upon receipt of the digital product identification, splitting, without retaining, the digital product identification into a plurality of digital product identification secret shares; upon receipt of the entity identification, splitting, without retaining, the entity identification into a plurality of entity identification secret shares; and sending the transaction identification, the plurality of digital product identification secret shares and the plurality of entity identification secret shares to at least one set of shareholders (see col.7, lines 17-59), wherein the anonymity service provider associatively stores the transaction identification with identifications of shareholders of the at least one set of shareholders (i.e., bank also stores the unique identifier, serial numbers and the address of seller, see col.8, lines 40-45).

Re claim 11. Krsul further discloses the method of claim 10, wherein the anonymity service provider communicates with the entity via a public communication network (i.e., world wide web, telephone network, see col.10, lines 52-55).

Re claim 12. Claim 12 recites similar limitations to claim 3, and thus rejected using the same art and rationale in the rejection of claim 3.

Re claims 13 and 14. Claims 13 and 14 recite similar limitations to claims 4 and 5 above, and thus rejected using the same art and rationale in the rejection of claims 4 and 5.

Re claim 15. Claim 15 recites similar limitations to claim 6 and thus rejected using the same art and rationale in the rejection of claim 6.

Re claim 16. The method of claim 10, further comprising: requesting, based on the stored transaction identification and identifications of shareholders, the plurality of digital product identification secret shares from the at least one set of shareholders (see col.9, lines 55-66); reconstructing the digital product identification based on the plurality of digital product identification secret shares (see fig.8 element 558); sending a digital product request comprising the digital product identification to a provider of the digital product (i.e., all buyer has to do is transmit each electronic token half to the seller's (provider of the digital product) computer network, see col. 9, lines 45-63), where in the anonymity service provider does not subsequently retain the digital product identification: receiving, in response to the digital product request, the digital product from the provider (see col.9, lines 60-63); requesting, based on the stored transaction identification and identifications of shareholders, the plurality of entity identification secret shares from the at least one set of shareholders (see col.9, lines 55-66); reconstructing the entity identification based on the plurality of entity identification secret shares (see fig.8 element 558); and sending the digital product to the entity based on the entity identification (seller releases the good and services to the buyer, see col.10 lines 45-55) wherein the anonymity service provider does not subsequently retain the entity identification (i.e., seller releases the desired goods and services to the to buyer, see col.10, lines 45-55)

Re claim 17. Claim 17 recites similar limitations to some of the limitations recited in claim 1, and thus rejected using the same art and rationale in the rejection of those limitations in claim 1.

Re claim 18. The method of claim 17, further comprising: receiving, from the entity, credit information; requesting, based on the stored transaction identification and identifications of shareholders, the plurality of purchase price secret shares (i.e., electronic token halves) from the additional set of shareholders (i.e., After making her selection and noting its price, see col.9, lines 55-63. Note that the electronic token has information about the price and the kind of goods and service being purchased etc); reconstructing the purchase price based on the plurality of purchase price secret shares (see fig.8 element 558); requesting, based on the stored transaction identification and identifications of shareholders (see col.9, lines 55-66), the plurality of entity identification secret shares from the at least one set of shareholders;

reconstructing the entity identification based on the plurality of entity identification secret shares (see fig.8 element 558); sending, based on the credit information, a credit verification request comprising the transaction identification, the entity identification, the purchase price and the credit information to a credit agency, wherein the anonymity service provider does not subsequently retain the entity identification, the purchase price and the credit information; receiving, from the credit agency, a credit approval identification and the transaction identification; requesting, based on the stored transaction identification and identifications of shareholders (see col.9, lines 55-66), the plurality of digital product identification secret shares from the at least one set of shareholders; reconstructing the digital product identification based on the plurality of digital product identification secret shares(see fig.8 element 558); sending the digital product identification and the credit approval identification to a clearing house in order to credit an amount equal to the purchase price to an account of the provider, wherein the anonymity service provider does not subsequently retain the digital product identification, the purchase price and the credit information (i.e., If bank 18 does not find a match, the seller is attempting to double spend the token, and bank 18 will not credit the seller for that electronic token. On the other hand, if the serial number of the electronic token matches a session serial number remaining in the relevant database entry, bank 18 removes the session serial number of the redeemed electronic token from the database entry and advances to step 1066. Bank 18 may also detect double spending using other approaches. Whatever approach is taken, bank 18 needs to ensure that it only honors an electronic token once. Once bank 18 determines that an electronic token is valid, however that is done, during step 1066 bank 18 increases the sum due to seller 17 by the amount of the electronic token. That done, bank 18 continues executing steps 1063 through 1066 until all of the seller's electronic tokens have been processed. When that occurs, during step 1068 bank 18 informs seller 17 of the credit to be given him and how that credit will be given to him, see col.11 lines 20-40).

Re claim 19. Claim 19 recites similar limitations to claim 1, and thus rejected using the same art and rationale in the rejection of claim 1.

Re claim 20. Claim 20 recites similar limitations to claim 2, and thus rejected using the same art and rationale in the rejection of claim 2.

Re claim 21. Claim 21 recites similar limitations to claim 10, and thus rejected using the same art and rationale in the rejection of claim 10.

Re claim 22. Claim 22 recites similar limitations to claim 11, and thus rejected using the same art and rationale in the rejection of claim 11.

Re claim 23. Claim 23 recites similar limitations to claim 16, and thus rejected using the same art and rationale in the rejection of claim 16.

Re claim 24. Claim 24 recites similar limitations to claim 17, and thus rejected using the same art and rationale in the rejection of claim 17.

Re claim 25. Claim 25 recites similar limitations to claim 18, and thus rejected using the same art and rationale in the rejection of claim 18.

A prior art on record, Bruce Schneier (Applied Crytography Second Edition, published by John Wiley &Sons, Inc. Copyright 1996), cited but not relied upon is pertinent to the present application in following ways: Schneier teaches different secret splitting schemes, one of which is the more complicated sharing scheme, called a threshold scheme, wherein you can take any message and divide it into n pieces, called shadows or shares amongst shareholders

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to OJO O. OYEBISI whose telephone number is (571) 272-8298. The examiner can normally be reached on 8:30A.M-5:30P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, HYUNG S. SOUGH can be reached on (571)272-6799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

HYUNG SOUGH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600

***